**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

I hereby certify that this correspondence is being transmitted via the Electronic Filing System (EFS) to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on,
June 8, 2009
(Date of Deposit)

Russell E. Fowler II
Name of person mailing Document or Fee

/Russell E. Fowler II/
Signature

June 8, 2009
Date of Signature

| Re: | | |
|---|---|---|
| | Application of: | Rhodes et al. |
| | Serial No.: | 10/671,234 |
| | Filed: | September 25, 2003 |
| | For: | Ethernet-Based Fire System Network |
| | Group Art Unit: | 2446 |
| | Confirmation No.: | 8197 |
| | Examiner: | Benjamin R. Bruckart |
| | Our Docket No.: | 2003P14811US (1867-0039) |

**BRIEF ON APPEAL**

Sir:

This is an appeal under 37 CFR § 41.31 to the Board of Patent Appeals and Interferences of the United States Patent and Trademark Office from the rejection of claims 1-20 of the above-identified patent application. Claims 1-20 have been finally rejected in an office action dated November 10, 2008. The fee of $540.00 is being pad herewith. Also, please provide any extension of time which may be necessary and charge any fees which may be due to Deposit Account No. 13-0014, but not to include any payment of issue fees.

**(1) REAL PARTY IN INTEREST**

Siemens Building Technologies is the owner of this patent application, and therefore the real party in interest.

**(2) RELATED APPEALS AND INTERFERENCES**

There are no related appeals or interferences in this case.

**(3) STATUS OF CLAIMS**

Claims 1-20 are pending in the application.

Claims 1-20 stand rejected and form the subject matter of this appeal. Claims 1-20 are shown in the Appendix attached to this Appeal Brief.

**(4) STATUS OF AMENDMENTS**

Applicants filed a Response to Office Action dated November 6, 2007 (hereinafter the "First Response") responsive to an Office Action dated August 6, 2007. The First Response included amendments to the claims which were entered by the examiner. A final Office Action dated December 28, 2007 was designated by the Examiner to be responsive to the First Response. On April 28, 2008, Applicants filed an RCE and claim Amendment (hereinafter the "RCE Amendment") that was responsive to the final Office Action. The Examiner entered the claims of the RCE Amendment and issued another office action dated July 2, 2008 (hereinafter the "Post RCE Office Action") responsive to the RCE Amendment. Applicants filed a Response to Office Action (hereinafter the "Post RCE Response") on October 2, 2008 that was responsive to the Post RCE Office action. The Examiner then

issued a final Office Action dated November 10, 2008 (hereinafter the "Second Final Action"), which was designated to be responsive to the Post RCE Response. Applicants filed a Notice of Appeal and Pre-Appeal Brief Request on February 10, 2009.

## (5) SUMMARY OF THE CLAIMED SUBJECT MATTER

An explanation of the subject matter defined in each of the independent claims involved in the appeal is provided below.

A. Independent Claim 1

Applicant's claimed invention, as set forth in independent claim 1, is directed to a "data transmission system for a facility". An exemplary portion of the specification showing the limitations of claim 1 is found at pages 17-18 of the specification, with reference to FIGs. 5 and 6. Furthermore, it should be noted that FIG. 3 shows a more detailed example of the system shown generally in FIG. 6. In the following summary of the claimed subject matter, exemplary reference numerals from FIG. 6 are provided first with related exemplary reference numerals from FIG. 3 provided at the end of each paragraph in brackets.

Claim 1 calls for "*a first network*". An exemplary "first network" is the fire control network 100 shown in FIGs. 5 and 6 and described at page 17, lines 7-23 of the specification. [*Also see* fire control network 10 of FIG. 3, with reference to page 18, line 23 to page 19, line 13 of the specification.]

Claim 1 also calls for "*a number of critical devices disposed within the facility*". The "critical devices" may be fire control devices, such as those shown in FIG. 1, and described at page 12, line 18 to page 13, line 12 of the specification. For example, the fire control devices may include initiating devices (such as smoke detectors 22 and pull switches 24) and

notification devices 26 (such as horns, strobes or speakers). [*Also see* IDC and NAC devices in FIG. 3.]

Claim 1 includes the further limitation of "*at least one first computer workstation operably coupled to said number of critical devices via said first network*". The "computer workstations" are shown in FIGs. 5 and 6 as fire control workstations 102 and 104. These fire control workstations 102 and 104 are described in the specification at page 17, lines 7-23. Further information concerning the fire control workstations can be found in the specification at page 10, line 21 to page 12, line 17, describing fire control workstations 12 and 13 of FIG. 1. [*Also see* fire control workstation 52' of FIG. 3, with reference to page 19, lines 3-11 and page 22, lines 3-17.]

Next, claim 1 calls for "*a second network including at least one second computer workstation*". "A second network" is shown in FIG. 6 as reference numeral 216, which includes a corporate network 218. "At least one second computer workstation" is shown in FIG. 6 by building control workstations 212 and 214. As explained at page 14, line 5 to page 15, line 15 of the specification, the building control workstations may be those that implement building automation software for a building automation network such as a network that controls the overall building environment by managing air handlers that supply heated or cooled air to a building. [*Also see* corporate network 75 and non-fire related workstation 71 in FIG. 3, with reference to page 20, lines 12-14 and page 22, lines 6-17.]

Finally, claim 1 calls for "*an isolating router coupling said first network to said second network and operable to isolate said first network from data transmission traffic in said second network, the isolating router comprising a router configured to receive and store data packets, and to forward the received data packets.*" An example of such an "isolating

router" is shown in FIG. 6 as reference numeral 224, and described at page 18, lines 7-18 of the specification. [Also see IP router 72 of FIG. 3, with reference to page 22, lines 6 to page 23, line 21.]

B. Independent Claim 8

Applicant's claimed invention, as set forth in independent claim 8, is directed to a "data transmission system for use in a facility." An exemplary portion of the specification showing the limitations of claim 1 is found at pages 19-23 of the specification, with reference to FIG. 3.

As shown in FIG. 3, the data transmission system comprises a first fire control Ethernet sub-network (10, 14) including a number of fire control devices (IDC, NAC, etc.). A number of fire safety workstations (52', 54') are operably coupled to said fire control devices and operable to implement software for maintaining and controlling said fire control devices (*see* p. 22, lines 5-20 of the specification).

FIG. 3 also shows a second building control Ethernet sub-network (50) including a number of building control devices (50, including TECs and UCs) and a number of building automation workstations (71) operably coupled to said building control devices (50) and operable to implement software for maintaining and controlling said building control devices (*see* p. 14, line 17 to p. 15, line 3 of the specification).

FIG. 3 also shows an isolating IP router (72) connecting said first sub-network to said second sub-network and operable to isolate said first network from data transmission traffic in said second network (*see* p. 22, lines 6-12 of the specification).

C. Independent Claim 14

Applicant's claimed invention, as set forth in independent claim 14, is directed to a data communication system for a facility. As shown in FIG. 3, the data communications system comprises a first network (10) and a second network (75) connected by an IP router (72). The first network (10) including a first plurality of work stations (52', 54') and the second network (75) including a second plurality of work stations (via 75). The first plurality of workstations include only building system workstations (52', 54'), and the second plurality of work stations include only non-fire safety related building system workstations and non-building system workstations (*see* p. 23, lines 9-15). The IP router (72) enables communication between the non-fire related building system workstations (via 75) and the first plurality of workstations (52', 54'). The IP router is also operable to disable communication between the non-building system workstations (via 75) and the first plurality of workstations (52', 54') (*see* p. 21, line 1 to p. 23, line 15).

**(6) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL**

Whether claims 1, 2, 4, 7, 14-17 are unpatentable under 35 U.S.C. §103(a) over U.S. Patent Publication No. 2003/0023874 to Prokupets et al. ("Prokupets") in view of U.S. Patent No. 5,815,664 to Asano ("Asano").

Whether claims 3 and 8-13 are unpatentable under 35 U.S.C. §103(a) over Prokupets et al in view of Asano and further in view of U.S. Patent Publication No. 2006/0114842 to Miyamoto et al. ("Miyamoto") in further view of U.S. Patent No. 6,144,736 to Koenig et al. ("Koenig").

Whether claims 5-6 and 20 are unpatentable under 35 U.S.C. §103(a) over Prokupets et al. in view of Asano in further view of Miyamoto et al.

Whether claims 18-19 are unpatentable under 35 U.S.C. §103(a) over Prokupets in view of Asano in further view of Koenig et al.

## (7) ARGUMENT

### I. The Rejection of Claims 1, 2, 4, 7, 14-17 under 35 U.S.C. §103(a) over Prokupets in view of Asano

#### A. Independent Claim 1

##### i. *Prokupets*

Prokupets is directed to a system for integrating security and access for facilities and information systems. As shown in Fig. 1, the Prokupets system shows an access control system, a surveillance system, a fire system and an intrusion detection system all connected via a network to a security server (*see* Prokupets at Abstract and Fig. 1).

##### ii. *Asano*

Asano is directed to an address reporting arrangement and method for detecting authorized and unauthorized addresses in a network environment. Asano addresses problem problems arising from a host computer having an authorized address trying to communicate with a host having an unauthorized address on another network (*see*, e.g., Asano at col. 2, lines 53-59). It is the object of Asano to enable a host having an authorized address to respond to a request from a host having an unauthorized address (*Id.* at col. 4, lines 26-38).

iii. *The Proposed Combination of Prokupets and Asano*

In the November 10, 2008 office action, the Examiner proposes a combination of Prokupets and Asano to arrive at the claimed invention. The examiner admits that Prokupets fails to teach the claimed router (*see* the Second Final Office Action at p.3, lines 1-2). However, in making this rejection in the Second Final Office Action, the Examiner made no mention of whether Prokupets includes "a second network" (*see* pages 2-3 of the Second Final Office Action). Indeed, based on the comments made in the response section of the Second Final Office Action, the Examiner now appears to consider the "second network" to be taught exclusively by Asano, and not to be found in Prokupets (*see* p. 11, line 15 of the Second Final Office Action where the examiner states, "The second network is taught by the Asano reference."). This position that the second network is found in Asano appears to be in response to Applicant's arguments in section II.E of Applicant's Post RCE Response that the network 20 of Prokupets can not constitute both the first network and the second network (*see* page 9, line 15 to page 11, line 14 of Applicant's Post RCE Response).

As set forth in the foregoing paragraph, it now appears that the examiner admits that Prokupets not only fails to teach the claimed "router", but also the "second network". The examiner attempts to address the shortcoming of Prokupets with respect to the router by citing teachings of Asano. In particular, the Examiner states that it would have been obvious to modify the apparatus of Prokupets to include "an isolating router that processes packets as taught by Asano in order to selectively enable communication between different networks" (see page 3, lines 9-12 and page 11, lines 24-29 of the Second Final Office Action).

iv. *The Proposed Combination does not Arrive at an the Isolating Router Coupling a First Network to a Second Network and Operable to Isolate the First Network From Data Transmission Traffic in the Second Network Device*

While the Examiner appears to have cited Asano as teaching "a second network" and the use of a "router", the Examiner has not identified with particularity how the second network and router would be used in the system of Prokupets. Thus, the Examiner has not identified a combination that arrives at the invention.

As argued by applicant in the Post RCE Response, the Examiner continues to assert the claimed first network is element 22c of Prokupets (*see* Second Final Office action at p.2). However, element 22c of Prokupets is a "fire system" (*see* Prokupets at Fig. 1 and ¶ [0024]). The fire system 22c of Prokupets is not a network, and the only network that appears to connect to the "fire system 22c" of Prokupets is the network 20. As a result, in the response section of the Second Final Office Action, the Examiner is now alleging that the network 20 constitutes the first network (see p.11, lines 11-12 of the Second Final Office Action). Still, the examiner continues to refer to fire system 22c as the "first network" in the actual rejection of claim 1 at page 2 of the Second Final Office Action. In view of this unclear position concerning the first and second networks, the Examiner's rejection in the Second Final Office Action is unclear and should be withdrawn. Nevertheless, for purposes of this Appeal Brief, it is assumed that the Examiner is alleging that the first network is the network 20, and that the second network is provided in Asano.

Admittedly, Fig. 1 of Prokupets has plenty of workstations. However, all of them appear to be connected to the network 20. Therefore, without identifying elements such as

the second workstation and second network in Prokupets, it is not possible to clearly articulate how the router of Asano would be inserted into the system of Fig. 1 of Prokupets. Indeed, in the Second Final Office Action, the examiner did not attempt to describe just how the router of Asano would be inserted into the system of FIG. 1 of Prokupets. Moreover, the Examiner does not identify with particularity how Prokupets would be modified, other than to "include an isolating router". The Examiner does not identify where the isolating router would be implemented. Further, because it is not clear what constitutes the claimed "networks" in Prokupets and Asano, one cannot speculate where such a router would be implemented.

As a consequence, it is respectfully submitted that merely including a router in the system of Prokupets does not arrive at the claimed invention. Moreover, the mere insertion of both a router and a second network in Prokupets does not arrive at the claimed invention. In particular, such inclusion, without more would not constitute "an isolating router coupling said first network to said second network and operable to isolate said first network from data transmission traffic in said second network, the isolating router comprising a router configured to receive and store data packets, and to forward the received data packets", as called for in claim 1.

v. *There is No Reason to Modify the Device of Prokupets to Include the Second Network and Isolating Router of Asano*

Even if the proposed modification did arrive at the claimed invention, the Examiner has not provided a clearly articulated and legitimate reason for making the proposed modification.

As best understood, the Examiner is alleging that it would be obvious to include an isolating router "in order to selectively enable communication between different networks" (*see* Second Final Office Action at p.11, lines 28-29). However, there is no reason to "selectively enable communication between different networks" in Prokupets. All communication in Prokupets appears to occur through the network 20. There does not appear to be separate networks in Prokupets through which communication can occur. As a consequence, one of ordinary skill in the art would not include an isolating router in Prokupets to "selectively enable communication between different networks". Furthermore, there is simply no reason to add a second network to Prokupets.

Even if there were two communication networks in Prokupets, nothing in either Prokupets or Asano suggests that these separate networks should be connected by a router, as opposed to a node that connects at another layer of the ISO protocol. To this end, it is noted that Asano does not stand for the proposition that a router should be used where a connection between networks is required. Instead, Asano teaches an address reporting device that may be used in situations in which a router is already implemented. (See, e.g. Asano background at col. 2, lines 10-32). Nothing in Asano teaches that a router is an advantageous way to connect any two networks. For example, if the two networks do not share physical characteristics (e.g. if both are not Ethernet), then a router cannot connect the networks.

Accordingly, Asano does not teach using a router to connect two different networks. Instead, Asano teaches that if the two networks are appropriate connectible using a router, then it would be advantageous to implement an address reporting device as disclosed. As a consequence, one of ordinary skill in the art would not have a reason to include a router in Prokupets to selectively enable communications between networks because nothing indicates

that a router would, in fact, selectively enable communications between any two networks in Prokupets.

Furthermore, Asano does not teach that a second network should be added where only a first network exists. As a consequence, one of ordinary skill in the art would not have a reason to include a second network in Prokupets.

vi. *Conclusion as to Claim 1*

In view of the foregoing, it is respectfully submitted that the obviousness rejection of claim 1 is in error for multiple reasons. For example, the proposed combination of Asano and Prokupets does not arrive at the invention because merely "including an isolating router" as proposed by the Examiner does not specify "an isolating router coupling said first network to said second network and operable to isolate said first network from data transmission traffic in said second network, the isolating router comprising a router configured to receive and store data packets, and to forward the received data packets", as claimed in claim 1. As also discussed above, there is no reason to incorporate a router between two networks in Prokupets because there does not appear to be two networks in Prokupets that could be connected via a router, and there is no reason to include the second network from Asano in Prokupets.

For at least these reasons, it is respectfully submitted that the rejection of claim 1 is in error and should be reversed.

B. Dependent Claim 2

Claim 2 depends from claim 1. In the rejection of claim 1 in the Second Final Office Action, the Examiner alleged that the network 20 of Fig. 2 of Prokupets constituted the claimed "first network" (*see* Final Office Action at p.11). Actually, the Examiner alleged

that the "Fire System 22c" of Prokupets constitutes the "first network" in page 2 of the office action, but then on page 11 alleges that the network 20 of Fig. 2 of Prokupets is the "first network". The Examiner appears to have redefined the identification of the "first network" in Prokupets in response to Applicants arguments in a prior response to office action (*see* Second Final Office Action at pp.10-11). In other words, in order to meet the requirements of claim 1, the Examiner admits that the claimed "first network" necessarily includes the network 20.

Claim 2 recites that "said first network is a fire control network". The network 20 of Prokupets, however, is not a "fire control network". It is a larger network that connects a fire system, an intrusion detection system, a surveillance system, and a building access control system to various servers. Such a network, which connects various non-fire systems to a fire system and other servers, is not a "fire control network" under any reasonable interpretation.

Nevertheless, in the rejection of claim 2, the Examiner again recites that the "fire system 22c" of Prokupets constitutes the claimed first network, and thus is a "fire control network" (*see* Second Final Office Action at p.3). However, this definition of the "first network" in connection with claim 2 inconsistent with the definition given in page 11 of the Second Final Office Action, which defines the first network as the network 20 of Prokupets.

Accordingly, the Examiner appears to use different and conflicting elements as the "first network", particularly when the "first network" as per underlying claim 1 is claimed to be a fire control network, as per claim 2. As a consequence, the obviousness rejection of claim 2 is in error and should be reversed.

C. Dependent Claim 4

Claim 4 recites, among other things, "a first Ethernet switch that meets one or more standards-issuing agencies publicly available standards for fire protective signaling uses". In the Second Final Office Action, the Examiner alleges that Koenig teaches this element at col. 17, lines 38-45. The cited passages do not teach anything that meets any standards relating to *fire protective signaling*. As discussed in the specification, fire protective signaling device standards specifically relate to fire safety systems (e.g. fire alarms and systems) (*see* specification of present application at p.11). The Examiner cites a device meeting a UL specification that is unrelated to *fire protective signaling use*. (See Koenig at col. 17, lines 38-45).

The Examiner has therefore failed to allege any teaching of "a first Ethernet switch that meets one or more standards-issuing agencies publicly available standards for fire protective signaling uses", particularly implemented as claimed in claim 4. As a consequence, the obviousness rejections of claim 4 should be reversed.

D. Dependent Claim 7

In the rejection of claim 7 in the Second Final Office Action, the Examiner alleged that "said isolating router is operable to block said broadcast transmissions to said first network" at page 1, paragraph 4 of Prokupets. However, paragraph 4 of Prokupets simply does not mention broadcast transmissions, much less blocking broadcast transmissions. The Examiner has therefore failed to establish where Prokupets and/or Asano teach the elements of claim 7. The rejection of claim 7 over Prokupets and Asano is therefore in error and should be reversed.

E. Independent Claim 14

Independent claim 14 also stands rejected as allegedly being obvious over Prokupets and Asano. Independent claim 14 is directed to a data communication system that includes: "*a first network and a second network connected by an IP router, the first network including a first plurality of work stations, the second network including a second plurality of work stations*".

Similar to claim 1, the Examiner has not identified where elements of the claim may be found in Prokupets or Asano. In particular, the Examiner has not identified "a first network and a second network". Furthermore, the Examiner has not identified a "first plurality of work stations" and "a second plurality of work stations" as claimed. The Examiner has, however, identified the database 26 and the client 30 as the second plurality of work stations (see Second Final Office Action at p.4). Accordingly, it may be assumed that the first plurality of work stations includes the elements 18a-18c of Prokupets, although this is never alleged. The elements 18a-18c are connected to the client 30 and the database 26 via the server 12. Accordingly, with these assumptions, it is further assumed that the Examiner is proposing replacing the server 12 with an IP router.

As discussed above in connection with claim 1, there is no reason to combine Prokupets and Asano such that the result includes a router to connect two different networks as there do not appear to be different networks in Prokupets. With respect to claim 14, the Examiner has identified elements 26 and 30 as possible other workstations coupled by other networks (see Second Final Office Action at p.6). Accordingly, it would appear that the Examiner is alleging that the network between the fire system 22c and the server 12 (network

20) constitutes the first "network" of Prokupets, and that the network between the server 12 and the database 26 and/or administration client 30 forms a second "network" of Prokupets.

Thus, the Examiner appears to argue that one of ordinary skill in the art would have a reason to place a router between the fire system 22c and the database 26 or client 30 of Prokupets. In other words, it appears that the Examiner is alleging that one would replace the server 12 of Prokupets with a router. Applicants respectfully disagree.

One of ordinary skill in the art would *not* replace the server 12 of Prokupets with a router. As discussed in previous office action responses, the server 12 executes applications that facilitate access of system data *stored in a database 14 within the server* to various network elements such as the database 26 and the client 30 (*see* Prokupets at ¶¶ [0037, 0039]). In other words, the database 26 and/or the client 30 do not interact directly with the fire system 22c such that the connection therebetween would include a router.

In particular, the server 12 Prokupets acts as a data server that coordinates the gathering and use of data from the systems 22a, 22b, 22c and 22d, which are then stored in a database 14 (*Id.* at ¶ [0021]). The server 12 allows other elements such as the database 26 and/or client 30 to access the database 14. Thus, the database 26 and/or server 30 are not effectively connected to the systems 22a, 22b, 22c and 22d at all. At best, the database 26 and/or server 30 are "connected" to the systems 22a, 22b, 22c and 22d at the *application layer*. Such a "connection" cannot be accomplished by replacing the application with "router". A router merely routes packets without any processing or coordination of the data within.

Accordingly, there is no reason to replace the server 12 with an IP router because it eliminate the main function of the server 12, which is central to the system of Prokupets.

One of ordinary skill in the art would have no reason to replace the server 12 with an IP router as appears to be proposed the Examiner.

For the foregoing reasons, it is respectfully submitted that the rejection of claim 14 over Prokupets and Asano is in error and should be reversed.

F. Dependent Claims 15-17

As set forth above, it is respectfully submitted that the rejection of independent claim 14 should be reversed. Accordingly, because dependent claims 15-17 depend from and incorporate all the limitations of independent claim 14, it is respectfully submitted that the rejection of dependent claims 15-17 under 35 U.S.C. § 103(a) should also be reversed.

## II. The Rejection of claims 3 and 8-13 under 35 U.S.C. §103(a) over Prokupets in view of Asano and further in view of Miyamoto and in further view of Koenig

A. Dependent Claim 3

Similar to claim 4 discussed above, claim 3 recites, among other things, "a first Ethernet switch that meets one or more standards-issuing agencies publicly available standards for fire protective signaling uses". In the Second Final Office Action, the Examiner alleges that Koenig teaches this element at col. 17, lines 38-45. The cited passages do not teach anything that meets any standards relating to *fire protective signaling*. As discussed in the specification, fire protective signaling device standards specifically relate to fire safety systems (e.g. fire alarms and systems) (*see* specification of present application at p.11). The Examiner cites a device meeting a UL specification that is unrelated to *fire protective signaling use*. (See Koenig at col. 17, lines 38-45).

The Examiner has therefore failed to allege any teaching of "a first Ethernet switch that meets one or more standards-issuing agencies publicly available standards for fire protective signaling uses", particularly implemented as claimed in claim 3. As a consequence, the obviousness rejections of claim 3 should be reversed.

B. Independent Claim 8

Independent 8 was rejected in the Second Final Office Action as allegedly being obvious over Prokupets and Asano in further view of Miyamoto. Independent claim 8 is directed to a data transmission system for use in a facility that includes "*an isolating IP router connecting said first [Ethernet] sub-network to said second [Ethernet] sub-network and operable to isolate said first network from data transmission traffic in said second network*".

As discussed above in connection with claim 1, there is no reason to combine Prokupets and Asano such that the result includes a router to connect two different networks as there do not appear to be different networks in Prokupets. However, in contrast to claim 1, the Examiner has identified elements 26 and 30 as possible other workstations coupled by other networks (see Second Final Office Action at p.6). Accordingly, it would appear that the Examiner is alleging that the network between the fire system 22c and the server 12 (network 20) constitutes the first "sub-network" of Prokupets, and that the network between the server 12 and the database 26 and/or administration client 30 forms a second "sub-network" of Prokupets.

Thus, the Examiner appears to argue that one of ordinary skill in the art would have a reason to place a router between the fire system 22c and the database 26 or client 30 of

Prokupets. In other words, it appears that the Examiner is alleging that one would replace the server 12 of Prokupets with a router. Applicants respectfully disagree.

As discussed previously with respect to independent claim 14, one of ordinary skill in the art would *not* replace the server 12 of Prokupets with a router. In particular, as discussed in Applicant's Post RCE Response, the server 12 executes applications that facilitate access of system data *stored in a database 14 within the server* to various network elements such as the database 26 and the client 30. (See Prokupets at ¶¶ [0037, 0039]). In other words, the database 26 and/or the client 30 do not interact directly with the fire system 22c such that the connection therebetween would include a router.

The server 12 Prokupets acts as a data server that coordinates the gathering and use of data from the systems 22a, 22b, 22c and 22d, which are then stored in a database 14. (*Id.* at ¶ [0021]). The server 12 allows other elements such as the database 26 and/or client 30 to access the database 14. Thus, the database 26 and/or server 30 are not effectively connected to the systems 22a, 22b, 22c and 22d at all. At best, the database 26 and/or server 30 are "connected" to the systems 22a, 22b, 22c and 22d at the *application layer*. Such a "connection" cannot be accomplished by replacing the application with "router". A router merely routes packets without any processing or coordination of the data within.

Accordingly, there is no reason to replace the server 12 with an IP router because it eliminate the main function of the server 12, which is central to the system of Prokupets. One of ordinary skill in the art would have no reason to replace the server 12 with an IP router as appears to be proposed the Examiner.

For the foregoing reasons, it is respectfully submitted that the rejection of claim 8 over Prokupets and Asano is in error and should be withdrawn.

C. Dependent Claims 9-13

As set forth above, it is respectfully submitted that the rejection of independent claim 8 should be reversed. Accordingly, because dependent claims 9-13 depend from and incorporate all the limitations of independent claim 8, it is respectfully submitted that the rejection of dependent claims 9-13 under 35 U.S.C. § 103(a) should also be reversed.

III. The Rejection of claims 5-6 and 20 under 35 U.S.C. §103(a) over Prokupets in view of Asano in further view of Miyamoto

As set forth above, it is respectfully submitted that the rejection of independent claim 1 should be reversed. Accordingly, because dependent claims 5-6 depend from and incorporate all the limitations of independent claim 1, it is respectfully submitted that the rejection of dependent claims 5-6 under 35 U.S.C. § 103(a) should also be reversed.

IV. The Rejection of claims 18-19 under 35 U.S.C. §103(a) over Prokupets in view of Asano in further view of Koenig

As set forth above, it is respectfully submitted that the rejection of independent claim 14 should be reversed. Accordingly, because dependent claims 18-19 depend from and incorporate all the limitations of independent claim 14, it is respectfully submitted that the rejection of dependent claims 18-19 under 35 U.S.C. § 103(a) should also be reversed.

**(8) CONCLUSION**

For all of the foregoing reasons, claims 1-20 are not unpatentable under 35 U.S.C. § 103(a). As a consequence, the Board of Appeals is respectfully requested to reverse the rejection of these claims.

This Appeal Brief is being filed within one month following the May 7, 2009 one month deadline to file an appeal brief in response to the Notice of Panel Decision form Pre-Appeal Review mailed April 7, 2009. Because the one month extension date for filing the Appeal Brief fell on Sunday, June 7, 2009, the Appeal Brief is being timely filed on Monday, June 8, 2009. Accordingly, applicant hereby petitions for a one month extension of time to file this response. Please charge the fees for such one month petition for extension of time to Deposit Account No. 13-0014.

Respectfully submitted,

/Russell E. Fowler II/

Russell E. Fowler II
Attorney for Applicants
Attorney Registration No. 43,615
Maginot Moore & Beck, LLP
Chase Tower
111 Monument Circle, Suite 3250
Indianapolis, Indiana 46204-5109
Telephone: (317) 638-2922

## CLAIM APPENDIX

1. (Previously presented) A data transmission system for a facility comprising:

a first network including;

a number of critical devices disposed within the facility;

and at least one first computer workstation operably coupled to said number of critical devices via said first network;

a second network including at least one second computer workstation; and

an isolating router coupling said first network to said second network and operable to isolate said first network from data transmission traffic in said second network, the isolating router comprising a router configured to receive and store data packets, and to forward the received data packets.

2. (Original) The data transmission system of claim 1, wherein:

said first network is a fire control network;

said number of critical devices include fire control devices; and

said first computer workstation implements software configured to receive data from and transmit data to said fire control devices.

3. (Previously presented) The data transmission system of claim 2, wherein said first network includes a first Ethernet switch that meets one or more standards-issuing agencies publicly available standards for fire protective signaling uses and that is operable to electrically isolate said first network from said isolating router.

4. (Previously presented) The data transmission system of claim 1, wherein:

said first network includes a first Ethernet switch that meets one or more standards-issuing agencies publicly available standards for fire protective signaling uses and that is operable to electrically isolate said first network from said isolating router; and

said isolating router meets one or more standards-issuing agencies publicly available standards for information technology equipment for fire protective signaling uses.

5. (Original) The data transmission system of claim 1, wherein said second network includes a building control network which includes a second Ethernet switch operably coupled to a number of building control devices independent of said operationally critical devices.

6. (Original) The data transmission system of claim 5, wherein:

said second network includes a corporate network, independent of said building control network, which includes workstations capable of broadcast transmissions; and

said isolating router is operable to block said broadcast transmissions to said first network.

7. (Original) The data transmission system of claim 1, wherein:

said second network includes a corporate network, independent of said first network, which includes workstations capable of broadcast transmissions; and

said isolating router is operable to block said broadcast transmissions to said first network.

8. (Previously presented) A data transmission system for use in a facility comprising:

a first fire control Ethernet sub-network including a number of fire control devices and a number of fire safety workstations operably coupled to said fire control devices and operable to implement software for maintaining and controlling said fire control devices;

a second building control Ethernet sub-network including a number of building control devices and a number of building automation workstations operably coupled to said building control devices and operable to implement software for maintaining and controlling said building control devices; and

an isolating IP router connecting said first sub-network to said second sub-network and operable to isolate said first network from data transmission traffic in said second network.

9. (Original) The data transmission system of claim 8, wherein said building automation workstations include a database server workstation and at least one database client workstation.

10. (Original) The data transmission system of claim 9, wherein database server workstation is connected within said first sub-network.

11. (Previously presented) The data transmission system of claim 10, wherein all workstations connected within said first sub-network meet more standards-issuing agencies publicly available standards fire protective signaling uses than at least some workstations connected outside the first sub-network.

12. (Previously presented) The data transmission system of claim 11, wherein said first sub-network includes a first Ethernet switch that meets one or more standards-issuing agencies publicly available standards for fire protective signaling uses.

13. (Previously presented) The data transmission system of claim 12, wherein said isolating IP router meets one or more standards-issuing agencies publicly available standards for information technology equipment for fire protective signaling uses.

14. (Previously presented) A data communication system for a facility comprising

a first network and a second network connected by an IP router, the first network including a first plurality of work stations, the second network including a second plurality of work stations, the first plurality of workstations including only building system workstations, the second plurality of work stations including only non-fire safety related building system workstations and non-building system workstations, and wherein the IP router enables communication between the non-fire related building system workstations and the first plurality of workstations, and the IP router is operable to disable communication between the non-building system workstations and the first plurality of workstations.

15. (Previously presented) The data communication system of claim 14 wherein at least one building system work station is a fire safety system workstation connected to one of a plurality of fire safety system devices.

16. (Previously presented) The data communication system of claim 14 wherein the first plurality of workstations includes at least one fire safety system workstation and at least one non-fire building system work station.

17. (Previously presented) The data communication system of claim 14 wherein at least one of the non-fire building system workstations is operably connected to heating ventilation and air conditioning system devices.

18. (Previously presented) The data communication system of claim 14 wherein the first network includes a switch that meets one or more standards-issuing agencies publicly available standards for fire protective signaling.

19. (Previously presented) The data communication system of claim 14 wherein the IP router meets one or more standards-issuing agencies publicly available standards for information technology equipment for fire protective signaling.

20. (Original) The data communication system of claim 1 wherein the first network comprises at least one Ethernet network and the second network comprises at least one Ethernet network.

# EVIDENCE APPENDIX

This section is empty

[NONE]

# RELATED PROCEEDINGS APPENDIX

This section is empty

[NONE]